



# Department of Homeland Security Daily Open Source Infrastructure Report for 04 January 2007

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Associated Press reports five employees of a baggage–handling contractor, Menzies Aviation Group, have been charged in the thefts of 158 pieces of luggage from George Bush Intercontinental Airport. (See item [10](#))
- The Department of Homeland Security on Wednesday, January 3, released scorecard assessments of interoperable communications capabilities in 75 urban and metropolitan areas nationwide. (See item [21](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *January 03, Cleveland Plain Dealer (OH)* — **PUCO wants gas utilities to check home pipes for leaks.** The Public Utilities Commission of Ohio (PUCO) has asked natural gas utilities to begin inspecting a section of customer gas lines for leaks that since 2000 have caused one death and \$970,000 in property damage in four fires. In a letter to Dominion East Ohio Gas Co., Columbia Gas of Ohio, and other utilities, PUCO Chairman Alan Schriber asked that workers begin an inventory and inspection of the gas line fixtures called "risers." The PUCO is developing an order to require such inspections. A riser is a section of pipe that connects a building's outdoor gas meter to the underground line that runs from the pipeline at the street.

Some designs are more prone to failure than others. A PUCO-ordered investigation revealed that the risers used in newer construction are often made of plastic — and that the plastic risers that are assembled on the spot by a contractor are often put together incorrectly or over-tightened. Over-tightening can distort gaskets and lead to leaks, especially during the winter and early spring when the ground repeatedly freezes and thaws. The report noted that "a failed plastic riser can blow full gas pressure against a structure and cause significant damage."

Source: <http://www.cleveland.com/printer/printer.ssf?/base/business/1167816801231720.xml&coll=2>

2. *January 02, Financial Times (UK)* — **U.S. reliance on OPEC highest in 15 years.** U.S. dependence on the Organization of the Petroleum Exporting Countries (OPEC) for its oil imports has risen to its highest level in 15 years, following Angola's arrival this week as the 12th member of the oil producers' group. Angola is the first new member to join the oil cartel since 1975. Including Angola, OPEC now supplies more than 54 per cent of the oil imports of the developed countries, its highest level for five years. For the U.S., the increase is even sharper: at more than 52 percent, OPEC's share of U.S. oil imports is at its highest since 1992. Important new fields developed by Total of France, Chevron, and Exxon Mobil of the U.S., and BP of the UK are either just coming on stream or are expected to begin producing in the next couple of years. However, Angola's entry into OPEC is unlikely to have much impact on the price of oil. It has yet to agree a production limit with the group, and OPEC officials have suggested that its planned production increase is likely to be accommodated by the group. As a result, the global balance of supply and demand is not expected to change.

Source: <http://www.ft.com/cms/s/50129e5e-9a88-11db-bbd2-0000779e2340.html>

3. *January 02, Electric Light & Power* — **Robotic crawler detects wear in power lines.** Most power companies don't know the weak points in their electrical grids. And although lights get turned on after a storm, the long-term effects of hurricanes, landslides or windstorms lie unnoticed. Now a robot can roll along the miles of cable, performing a utilities' equivalent of check-ups. "This is the first robot built that can inspect power cables autonomously looking for incipient failures," says University of Washington (UW) assistant professor Alexander Mamishev. "It can find cables that may need repair, before they cause problems." The high-voltage lines that this robot monitors carry electricity from the distribution plant to the substations. UW's robot can pinpoint problem spots by using information from the surface of the cable to assess the condition of what's inside. The robot rides along the insulated distribution cable scanning for internal damage. It uses three sensors: a heat sensor that detects heat dissipation; an acoustic sensor that listens for partial electrical discharge; and a sensor that detects "water trees," filaments of water that have seeped into insulation. Engineers monitor the robot via wireless connection and watch through a video camera.

Source: [http://uaelp.pennnet.com/display\\_article/281106/22/ARTCL/non e/none/Robotic-crawler-detects-wear-in-power-lines/](http://uaelp.pennnet.com/display_article/281106/22/ARTCL/non e/none/Robotic-crawler-detects-wear-in-power-lines/)

4. *January 02, Associated Press* — **Twelve months after Sago, coal industry still changing.** Many of the safety measures state legislatures and Congress rushed to adopt to protect the 46,000 people working in the nation's underground coalmines after the January 2, 2006, Sago Mine explosion have yet to take effect. There are still no rescue chambers or wireless tracking and communications equipment in the country's 606 underground coalmines, and it's unlikely there will be until federal requirements kick in more than two years from now. Hundreds of

emergency air packs that are to be stored underground — though currently required by law — are on backorder and will take months to deliver. Other safety improvements seem to be stalling altogether. West Virginia's August deadline for mines to submit plans for high-tech wireless communications has come and gone.

Source: <http://www.chron.com/disp/story.mpl/business/energy/4438528.html>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

5. *January 02, WBNS-10TV (OH)* — **Nitrogen oxide plume prompts evacuations.** A plume of red and yellow smoke brought the Columbus, OH, Fire Department, Hazmat crews and the Environmental Protection Agency to a west Columbus chemical plant Tuesday afternoon, January 2. Officials say someone at GFS Chemicals mixed an acid and a base together, and that released nitrogen oxide into the air from a plant smokestack. The plume only lasted about a minute. There were some evacuations, primarily from businesses across the street from GFS. No one was injured.

Source: <http://www.10tv.com/?sec=news&story=sites/10tv/content/pool/200701/1750749304.html>

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

6. *January 02, Federal Computer Week* — **DoD programs plagued by immature technology.** The Army has moved major programs forward despite a lack of critical technologies, a problem that causes delays and cost overruns and sometimes makes it impossible to provide service members with capabilities they need, according to David Walker, comptroller general at the Government Accountability Office (GAO). The programs were based on unrealistic expectations and suffer from a lack of accountability and oversight, Walker said. Information technology systems, such as the Future Combat System and the Warfighter Information Network-Tactical, were among the many programs that Walker identified as being ahead of their core technologies. Walker detailed his criticisms in writing on December 21 in response to questions posed by the House Defense Appropriations Subcommittee. He had testified before the subcommittee on September 7. The Department of Defense (DoD) should separate technology development from system development to reduce risks, Walker said. Programs with immature technology see cost growth averaging 35 percent, compared to 5 percent cost growth in programs with mature technologies, he noted.

Source: <http://www.fcw.com/article97225-01-02-07-Web>

7. *January 02, Federal Times* — **Defense IG faults contracting through Treasury.** The Department of Defense (DoD) failed to follow procedure in some purchases through a Department of the Treasury fund, the Pentagon's Office of the Inspector General (IG) found. An IG audit reviewed 61 orders worth about \$37.8 million that DoD placed through Treasury's FedSource franchise fund in fiscal 2005. In all 61 cases, Defense contracting officers failed to conduct market research to identify vendors able to meet their agency's needs, auditors found.

Approximately 85 percent of the orders failed to show prices were reasonable, had inadequate interagency agreements and had inadequate contractor oversight plans. More than 67 percent of orders lacked competition, according to the December 8 report released December 26.

Report: <http://www.dodig.mil/Audit/reports/FY07/07-032.pdf>

Source: <http://federaltimes.com/index.php?S=2455921>

[\[Return to top\]](#)

## **Banking and Finance Sector**

8. *January 02, Finextra (UK)* — **Identity Theft Task Force calls for public input.** The President's Identity Theft Task Force announced that it is seeking public comment on various possible recommendations to improve the effectiveness and efficiency of the federal government's efforts to reduce identity theft. In preparing to produce a final strategic plan to the President, the Task Force is considering, among other things, various ways to improve the coordination and effectiveness of criminal prosecution of identity theft, to enhance data protection for sensitive consumer information maintained by the public sector, private sector, and the consumer himself or herself, and to provide more comprehensive and effective guidance for consumers and the business community. The Task Force also is considering ways to improve recovery and assistance for consumers following a breach or misuse of their information. Comments must be filed on or before Friday, January 19, 2007.

Source: <http://www.finextra.com/fullpr.asp?id=12715>

9. *January 02, 6 WDSU (LA)* — **FBI warns about Road Home scam.** The FBI is warning southeast Louisiana residents about a Road Home scam that could be a very pricey mistake for homeowners. Con artists are making calls and offering phony federal grants that they claim can be repaid once the Road Home money is dispersed, officials said. However, homeowners are asked to pay a \$300 processing fee and give credit card and bank account numbers. The scammers then run up the credit card bills and drain their victims' bank accounts.

Source: [http://news.yahoo.com/s/wdsu/20070102/lo\\_wdsu/10654922](http://news.yahoo.com/s/wdsu/20070102/lo_wdsu/10654922)

[\[Return to top\]](#)

## **Transportation and Border Security Sector**

10. *January 03, Associated Press* — **Five charged in Texas airport luggage thefts.** Five employees of a baggage-handling contractor, Menzies Aviation Group, have been charged in the thefts of 158 pieces of luggage from George Bush Intercontinental Airport, police said Tuesday, January 2. Sixty-eight pieces of luggage were discovered in a Houston pet store's trash bin on December 26. Police said the luggage appeared to have been picked over, with any valuables stolen. Another 90 pieces of stolen luggage were found at two undisclosed locations over the weekend, Houston Police Capt. Rick Bownds said. Charged with engaging in organized criminal activity were twin brothers Manuel and Ricardo Aguilar, 23; Carlos Osorio, 24; Erick Perez, 29; and Daniel Venegas, who turns 26 this week. The Aguilar brothers, Osorio and Perez were being held at the Harris County Jail on \$20,000 bond. Information was not available for Venegas.

Source: [http://www.usatoday.com/news/nation/2007-01-02-lost-luggage\\_x.htm](http://www.usatoday.com/news/nation/2007-01-02-lost-luggage_x.htm)

11. *January 03, Associated Press* — **Airports near Los Angeles hope using big city's name will boost use.** Regional airports outside Los Angeles are hoping they can boost use of their facilities by adopting the big city's moniker — a move officials say has been effective in other states. Los Angeles' Airport Commission voted last month to change the name of Ontario's airport to LA/Ontario International Airport and Palmdale's facility to LA/Palmdale Regional Airport. Officials hope aligning the airports with a well-known geographic hook will draw travelers from outside California, encourage airlines to offer more flights at the facilities and take the pressure off aging Los Angeles International Airport. "Adding 'LA' to the Palmdale and Ontario airports conveys locally that there is a larger regional system for air transportation, better identifies the size of the Los Angeles region, and creates a better linkage between Palmdale and the Los Angeles basin," said Palmdale Mayor Jim Ledford, in a statement. This month airlines will submit proposals to offer flights from Palmdale, located about 65 miles north of LAX in the Antelope Valley. Los Angeles airport officials are also in negotiations to land major new air service at Ontario, about 40 miles east of downtown Los Angeles.

Source: [http://www.usatoday.com/travel/news/2007-01-02-california-airports\\_x.htm](http://www.usatoday.com/travel/news/2007-01-02-california-airports_x.htm)

12. *January 03, Associated Press* — **Ocean scoured for Indonesia jet.** Rescuers scoured the ocean for a missing jetliner Wednesday, January 3, one day after senior Indonesian officials erroneously said the Boeing 737's charred wreckage had been found in a remote mountainous area and that a dozen people may have survived. Three navy ships set sail soon after sunrise in the Makassar Strait and five air force planes took off to search for signs of wreckage, said Bambang Karnoyudho, head of the National Search and Rescue Agency. Karnoyudho said that based on radar and satellite readings, he thought it most likely that the plane had fallen into the sea. Adam Air Flight KI-574, carrying 102 people, was flying from Indonesia's main island of Java to North Sulawesi's provincial capital of Manado when it disappeared Monday in stormy weather after sending out distress signals — one over mountainous jungles and the other along the coast.

Source: <http://www.cnn.com/2007/WORLD/asiapcf/01/03/indonesia.plane.ap/index.html>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

[\[Return to top\]](#)

## **Agriculture Sector**

13. *December 30, Associated Press* — **Three California tracks under equine herpes quarantine.** Three thoroughbred racetracks in California's San Francisco Bay area were placed under quarantine Friday, December 29, after a thoroughbred at Golden Gate Fields tested positive for the equine herpes virus. Under the quarantine, horses may be transferred between Golden Gate in Albany, Bay Meadows in San Mateo and Pleasanton, but no horse may leave any of the tracks except to travel to another quarantined track, according to the California Horse Racing

Board. The length of the quarantine will depend on the tracks' ability to contain the spread of the infection, which has so far only involved one horse. This year, similar outbreaks affected tracks in New Jersey, Maryland and Kentucky.

Equine herpes information: <http://www.vet.uga.edu/vpp/IVM/ENG/ERD/EHV-4and1.html>

Source: <http://sports.espn.go.com/sports/horse/news/story?id=2714982>

14. *December 29, Casper Star Tribune (WY)* — **Disease rate rises in elk.** A new report shows the level of brucellosis exposure in Wyoming's Buffalo Valley elk has jumped during a period when emergency feeding of the animals took place. The emergency feeding began several years ago when deep snow prevented elk from leaving the area near cattle and prevented managers from moving elk. Eric Keszler with the Wyoming Game and Fish Department said no permanent feedground is going to be established in the Buffalo Valley. Low snow levels in northwest Wyoming this winter have allowed wildlife managers to haze elk away from cattle lines in the Buffalo Valley, and no emergency feeding has been necessary. The new report examining abortion and birth rates in the brucellosis-endemic area of Wyoming said seroprevalence rates jumped significantly for elk in the Buffalo Valley. Seroprevalence shows an animal has been exposed to the brucellosis bacteria but does not necessarily have the disease, which can cause ungulates to abort. Brucellosis exposure rates had been estimated to be just more than two percent in the Buffalo Valley elk, but recent surveys put the number at 20 percent.

Brucellosis information: <http://www.aphis.usda.gov/vs/nahps/brucellosis/>

Source: <http://www.casperstartribune.net/articles/2006/12/29/news/wyoming/4d96463e413b8e508725725200006a38.txt>

[\[Return to top\]](#)

## **Food Sector**

15. *January 03, Associated Press* — **South Korea, U.S. to discuss beef quarantine dispute.**

South Korea and the U.S. will hold talks next week on a dispute over South Korea's decision to reject American beef shipments that it said contained banned bone fragments, South Korean officials said Wednesday, January 3. The talks scheduled for Monday, January 8, and Tuesday, January 9, in Seoul come weeks after South Korea rejected all three recent shipments of American beef because of bone fragments that South Korea fears could potentially harbor mad cow disease. The two sides will "hold technical consultations" over the quarantine issue of American beef, said a South Korean Agriculture and Forestry Ministry official. South Korean officials said they discovered unacceptable levels of the dioxin in the third American beef shipment. Seoul has asked Washington to explain why the beef contained the toxic chemical, but the U.S. has given no answer yet, according to the ministry.

Source: <http://www.cattlenetwork.com/content.asp?contentid=94778>

16. *January 03, Food Production Daily* — **Allied Bakeries hit by new round of malicious tampering.** The United Kingdom's Allied Bakeries' Kingsmill sliced bread brand has been hit with a new round of sabotage. The UK's food regulator the Food Standards Agency (FSA) on December 21 said it was urging consumers to be vigilant after further suspected cases of malicious tampering were discovered. Deliberate sabotage of a product is a plant manager's nightmare, one that Allied Bakeries has been having over the past 18 months. The new



incidents came to light after customers reported discovering foreign objects in loaves of the Kingsmill sliced bread. In one incident, pieces of glass were reported to be found inside the packaging and not embedded in the bread. Three further incidents are currently being investigated by the police to see if they are linked to an ongoing investigation. The bakery distributes to retailers, including supermarkets and smaller outlets, across the south east of England. Over the last 18 months, the FSA has been working with the police to discover the culprit. In the past Allied Bakeries has reported at least five deliberate cases of malicious tampering of its Kingsmill brand. Police have so far not determined whether the tampering is happening inside the factory or in the supply chain.

Source: <http://www.foodproductiondaily.com/news/ng.asp?n=73037-allied-bakeries-kingsmill-tampering>

[[Return to top](#)]

## **Water Sector**

Nothing to report.

[[Return to top](#)]

## **Public Health Sector**

17. *January 02, National Institutes of Health* — **Vaccine for H5N1 avian influenza enters human trial.** The first human trial of a DNA vaccine designed to prevent H5N1 avian influenza infection began on December 21, 2006, when the vaccine was administered to the first volunteer at the National Institutes of Health (NIH) Clinical Center in Bethesda, MD. Scientists from the Vaccine Research Center (VRC) at the National Institute of Allergy and Infectious Diseases (NIAID), one of the NIH Institutes, designed the vaccine. Unlike conventional flu vaccines, which are developed by growing the influenza virus in hens' eggs and then administered as a weakened or killed form of the virus, DNA-based vaccines contain only portions of the influenza virus' genetic material. Once inside the body, the DNA instructs human cells to make proteins that act as a vaccine against the virus. The DNA vaccine used in this study is similar to other investigational vaccines evaluated by the VRC that hold promise for controlling other viruses, such as HIV, Ebola, SARS and West Nile. The candidate vaccine, synthesized using a modified version of the hemagglutinin (H) gene from the H5N1 influenza virus, was manufactured at the VRC Vaccine Pilot Plant. This is the first VRC candidate vaccine manufactured at the VRC Vaccine Pilot Plant.

Source: <http://www.nih.gov/news/pr/jan2007/niaid-02.htm>

18. *December 29, National Institute of Arthritis and Musculoskeletal and Skin Diseases* — **Molecular anatomy of influenza virus detailed.** Scientists at the National Institute of Arthritis and Musculoskeletal and Skin Diseases (NIAMS) and colleagues at the University of Virginia have succeeded in imaging, in unprecedented detail, the virus that causes influenza. A team of researchers working with a version of the seasonal H3N2 strain of influenza A virus, has been able to distinguish five different kinds of influenza virus particles in the same isolate (sample) and map the distribution of molecules in each of them. This breakthrough has the potential to identify particular features of highly virulent strains, and to provide insight into how antibodies

inactivate the virus, and how viruses recognize susceptible cells and enter them in the act of infection. One of the difficulties that has hampered structural studies of influenza virus is that no two virus particles are the same. In this fundamental respect, it differs from other viruses. The research team used electron tomography (ET) to make its discovery. ET is a novel, three-dimensional imaging method based on the same principle as the well-known clinical imaging technique called computerized axial tomography, but it is performed in an electron microscope on a microminiaturized scale.

Source: [http://www.niams.nih.gov/ne/press/2006/12\\_29.htm](http://www.niams.nih.gov/ne/press/2006/12_29.htm)

[\[Return to top\]](#)

## **Government Sector**

19. *January 03, Associated Press* — **Teen arrested in Tacoma school shooting.** A teenager was shot to death in a high school hallway on Wednesday as classes resumed after the winter break, and police arrested a fellow student found wandering a neighborhood a few miles away, authorities said. Police were trying to determine what prompted the shooting. Witnesses said the gunman fired three shots at point-blank range, splattering blood on lockers at Foss High School in Tacoma, WA, and setting off panic. He did not appear to be aiming at anyone other than the victim. The teenager suspected in the shooting was caught without incident about two hours later in a suburban area dotted with homes and shopping centers. The identities of the two students were not immediately released. The school was locked down after the shooting. Classes were canceled for the rest of the day and students sent home about an hour later.

Source: <http://www.chron.com/disp/story.mpl/ap/nation/4441960.html>

[\[Return to top\]](#)

## **Emergency Services Sector**

20. *January 03, Contra Costa Times (CA)* — **Agents work to keep disaster teams safe.** When levees collapsed and the Louisiana Superdome swelled with the displaced and despairing, federal officials sent a Bay Area, CA, medical team to help the sick and dying. But with scant security and a crowd in the tens of thousands growing rowdier, and in some cases violent amid the rank swelter, conditions proved too perilous for the volunteer doctors, nurses and medical staff. It's a scenario of chaos that could well repeat itself in California, say disaster doctors and planners. And it's one that a group of state Department of Justice (DoJ) agents is working to prevent by creating a security and logistics force to protect disaster medical teams and their supply caches. They are now setting up dozens of teams across the state to scout triage sites, equipping themselves with rugged vehicles, contamination suits, rescue gear and health supplies in case catastrophe strikes. The new teams would focus on one task — protecting medical professionals. It's a role that the Highway Patrol or local police agencies might take, but in a catastrophe other tasks may overwhelm them, said Dale Ferranto, assistant director of the DoJ's firearms division.

Source: <http://www.contracostatimes.com/mld/cctimes/news/16372950.htm>

21.



*January 03, Department of Homeland Security* — **DHS releases nationwide interoperable communications assessment.** The Department of Homeland Security (DHS) on Wednesday, January 3, released scorecard assessments of interoperable communications capabilities in 75 urban and metropolitan areas nationwide. Interoperable communications involve policies, technology and training that enable law enforcement, fire and emergency medical services from multiple jurisdictions in a common community to effectively communicate within one hour of an incident. Key findings include: a) Policies for interoperable communications are now in place in all 75 urban and metropolitan areas; b) Regular testing and exercises are needed to effectively link disparate systems and facilitate communications between multi-jurisdictional responders (including state and federal); c) Cooperation among first responders in the field is strong, but formalized governance (leadership and strategic planning) across regions is not as advanced.

Summary Report and Findings: <http://www.dhs.gov/xlibrary/assets/grants-scorecard-report-010207.pdf>

Scorecard results by State area: [http://www.dhs.gov/xprepresp/gc\\_1167767584358.shtm](http://www.dhs.gov/xprepresp/gc_1167767584358.shtm)

Tactical Interoperability Communication Scorecards:

[http://www.dhs.gov/xprepresp/gc\\_1167770109789.shtm](http://www.dhs.gov/xprepresp/gc_1167770109789.shtm)

Score definitions: [http://www.dhs.gov/xprepresp/gc\\_1167767584358.shtm#legend](http://www.dhs.gov/xprepresp/gc_1167767584358.shtm#legend)

Source: [http://www.dhs.gov/xnews/releases/pr\\_1167843848098.shtm](http://www.dhs.gov/xnews/releases/pr_1167843848098.shtm)

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

22. *January 03, Sophos* — **Top ten malware threats and hoaxes reported to Sophos in December 2006.** Sophos has revealed the most prevalent malware threats and e-mail hoaxes causing problems for computer users around the world during December 2006. The figures show that the long-established Dref malware has made an unexpected return to the top of the threat chart, thanks to two new variants currently causing problems for computer users worldwide. The Dref-V mass-mailing worm, which poses as a New Year e-card, was discovered on December 30, 2006, and by the following day accounted for 93.7 percent of infected e-mails. As a result, Dref — which was first seen in July 2005 — has knocked last month's main offender Stratio (also known as Stration) off the top of the chart. Stratio, currently in fourth place, now accounts for just 7.8 percent of the total. The proportion of infected e-mail continues to remain low, at just one in 337 (0.30 percent), while during December Sophos identified 6,251 new threats, bringing the total number of malware protected against to 207,684. Refer to source to view the full report.

Source: [http://www.sophos.com/pressoffice/news/articles/2007/01/topt\\_endec.html](http://www.sophos.com/pressoffice/news/articles/2007/01/topt_endec.html)

23. *January 02, eWeek* — **Month of Apple Bugs, meet Month of Patches.** It's officially a cat-and-mouse race to exploit — and fix — security vulnerabilities affecting Apple Computer's Mac operating system. Less than 24 hours after the release of working exploits for two critical media player flaws — QuickTime and VLC — a former engineer in Apple's BSD Technology Group has launched an effort to provide run-time fixes for each flaw released during the Month of Apple Bugs (MoAB) project. Landon Fuller, one of the primary architects of the Darwin ports system, has announced plans to react to each MoAB bug with a daily, unofficial patch.

Source: <http://www.eweek.com/article2/0.1895.2078433.00.asp>

24. *January 02, eWeek* — **Survey: Consumers not confident about Internet security.** Trend Micro on Tuesday, January 2, released the Internet Confidence and Safety survey that evaluates consumers' attitudes about Internet-related concerns such as how safe they feel when using the Internet, their opinions regarding the future of Internet security, their experience with Internet infections and their confidence when it comes to security software. The study, which was gathered in September 2006 and will take place at six-month intervals in Japan, the United States, the United Kingdom, Germany and France, reported that 51 percent of consumers are not confident that their Internet security software is protecting their system. The study also found that while 51 percent of respondents in the United States feel that the Internet is very safe, 32 percent feel that the Internet will be less safe in six months. The new research study from Trend Micro concluded that consumers take part in what is considered risky online behavior by participating in online banking, using credit cards to buy things and downloading freeware or shareware.

Survey results: [http://www.trendmicro.com/en/about/news/pr/archive/2006/pr01\\_0207.htm](http://www.trendmicro.com/en/about/news/pr/archive/2006/pr01_0207.htm)

Source: <http://www.eweek.com/article2/0.1895.2078315.00.asp>

25. *January 02, IDG News Service* — **Google closes Gmail cross-site scripting vulnerability.** Google Inc. has fixed a flaw that would have allowed Websites to harvest information from Gmail contact lists, a problem that could have let spammers collect reams of new e-mail addresses. For an attack to work, a user would have to log into a Gmail account and then visit a Website that incorporates JavaScript code designed to take contact information from Gmail. Proof-of-concept code was publicly posted.

Source: [http://www.infoworld.com/article/07/01/02/HNgmailscripting\\_1.html](http://www.infoworld.com/article/07/01/02/HNgmailscripting_1.html)

26. *January 02, IDG News Service* — **Outage knocks Lycos offline.** A network outage at hosting provider SAVVIS Communications has knocked a number of Websites offline, including Web portal Lycos. The outage occurred around 9 a.m. Eastern on Tuesday morning, December 2, when a backup data line connecting SAVVIS's Boston data centers was accidentally severed, said Kathy O'Reilly, a Lycos spokesperson. At the time, crews had been in the process of repairing the main line to the data center, which was also down, she added. With the two data lines out of service, the entire Lycos Network including Lycos Mail and the Tripod Web hosting service was knocked off the Internet, O'Reilly said. None of the data being stored by Lycos was affected by the incident, she added.

Source: [http://www.infoworld.com/article/07/01/02/HNsavvis\\_1.html](http://www.infoworld.com/article/07/01/02/HNsavvis_1.html)

27. *January 02, Washington Technology* — **DHS plans IT employee records database.** The Department of Homeland Security (DHS) is setting up a new records system to keep track of the names, passwords, citizenship information and other data on thousands of IT workers with access to the department's systems. In a notice posted December 29, DHS announced it is creating a new sensitive, but unclassified, database as part of its General Information Technology Access Account Records System. The new database will collect personal information from IT employees, contractors, grantees and others, including people who serve on DHS advisory committees or are listed as points of contact for facilities.

Source: [http://www.washingtontechnology.com/news/1\\_1/daily\\_news/29923-1.html?topic=homeland](http://www.washingtontechnology.com/news/1_1/daily_news/29923-1.html?topic=homeland)

## Internet Alert Dashboard

### Current Port Attacks

<b>Top 10 Target Ports</b>	4662 (eDonkey2000), 1026 (win-rpc), 2967 (ssc-agent), 25 (smtp), 4672 (eMule), 80 (www), 5677 (---), 1433 (ms-sql-s), 139 (netbios-ssn), 445 (microsoft-ds)
----------------------------	---

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## Commercial Facilities/Real Estate, Monument & Icons Sector

**28. *January 03, Washington Post* — From monitoring teens to minding terrorists.** The job of a shopping mall security guard normally involves controlling rowdy teenagers, finding lost children and patrolling parking lots. But starting this month, malls across the country will begin training guards for another task: fighting terrorism. The 14-hour program is being developed by the International Council of Shopping Centers, a trade group, and the Homeland Security Policy Institute at George Washington University in Washington, DC, at a cost of \$2 million. It is the first standardized anti-terrorism curriculum written for the nation's estimated 20,000 mall security guards. Developers of the program say it is crucial to safeguarding shopping centers, which have significant economic import — as evidenced by the billions of dollars spent at malls during the holiday season — and have emerged as modern-day town centers, with movie theaters, restaurants, and now grocery stores and gyms. The training focuses on making guards more aware of the effects of terrorist attacks and helping them recognize potential attackers. It ranges from the understanding the characteristics of the nerve agent sarin (especially dangerous in enclosed spaces because it vaporizes quickly) to spotting suicide bombers (look for unusual dress, like a heavy coat in the middle of summer).

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/02/AR2007010201094.html?sub=AR>

[[Return to top](#)]

## General Sector

Nothing to report.

[[Return to top](#)]

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.